PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-215165
(43)Date of publication of application : 04.08.2000

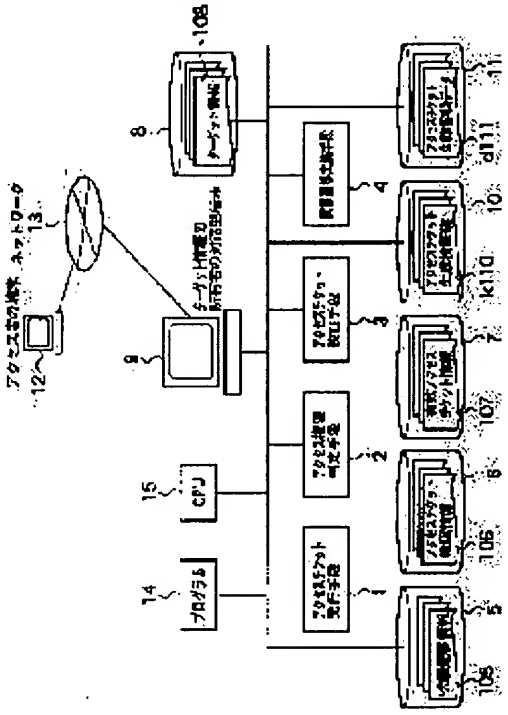
(51)Int.Cl. G06F 15/00
G06F 12/14
G06F 17/60
G09C 1/00
H04L 9/32

(21)Application number : 11-017401
(22)Date of filing : 26.01.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : OSHIMA YOSHITO
OHARA YASUHIRO

(54) METHOD AND DEVICE FOR INFORMATION ACCESS CONTROL AND RECORD MEDIUM RECORDING INFORMATION ACCESS CONTROL PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the method and device for information access control which can easily change the access authority to be allowed to an accessing person in response to the change of situation of a transaction and also to provide a recording medium which records an information access control program.
SOLUTION: An access ticket issuing means 1 issues the access tickets to every accessing person and these tickets prescribe the access authority to the target information for each of plural types and states. Receiving an access request from an accessing person, the means 1 reads the request and the access authority corresponding to the type and state of an inputted access ticket out of an access ticket authority information storing means 6 and decides to permit or not permit the access request based on the access authority. When a state transition request is received from the accessing person, the transition destination state is read out of a state transition information storing means 5 based on the type and state of the access ticket that is inputted together with the state transition request. Based on the transition destination state, the change of the access ticket is updated.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－215165
（P2000－215165A）
(43)公開日　平成12年８月４日(2000.8.4)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
G06F	15/00	330	G06F	15/00	330A	5B017
	12/14	310		12/14	310K	5B049
	17/60		G09C	1/00	660E	5B085
G09C	1/00	660	G06F	15/21	Z	5J104
H04L	9/32		H04L	9/00	671	9A001

審査請求　未請求　請求項の数24　ＯＬ　（全 23 頁）

(21)出願番号　特願平11－17401

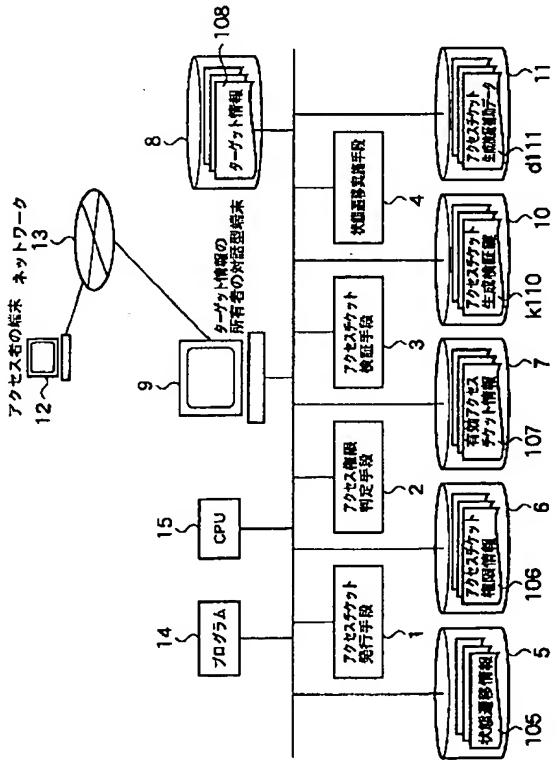
(22)出願日　平成11年１月26日(1999.1.26)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　大鳴　嘉人
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　大原　康博
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】　情報アクセス制御方法および装置と情報アクセス制御プログラムを記録した記録媒体

(57)【要約】
【課題】　アクセス者に対して許容するアクセス権限を取引の局面で変化に応じて容易に変更することができる情報アクセス制御方法および装置と情報アクセス制御プログラムを記録した記録媒体を提供する。
【解決手段】　アクセスチケット発行手段１で複数の種類の複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス者からのアクセス要求を受け付けると、この要求とともに入力されたアクセスチケットの種類および状態に対応するアクセス権限をアクセスチケット権限情報格納手段６から読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付けると、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を状態遷移情報格納手段５から読み出し、この遷移先状態でアクセスチケットの状態を更新する。



1

【特許請求の範囲】

【請求項１】　保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御方法であって、

複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、

アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、

アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを特徴とする情報アクセス制御方法。

【請求項２】　保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御方法であって、

アクセスの内容に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、

アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、

アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを特徴とする情報アクセス制御方法。

【請求項３】　前記アクセスチケットの状態を更新する処理は、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して状態遷移情報格納テーブルに格納しておき、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新することを特徴とする請求項１記載の情報アクセス制御方法。

【請求項４】　前記アクセスチケットの状態を更新する処理は、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して状態遷移情報格納テーブルに格納しておき、アクセス者から前記状態遷移要求とともに入力されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新することを特徴とする請求項２記載の情報アクセス制御方法。

2

【請求項５】　前記アクセスチケットの状態を更新する処理は、アクセス者からの前記状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して前記遷移先状態を決定していることを特徴とする請求項１乃至４のいずれかに記載の情報アクセス制御方法。

【請求項６】　前記要求とともに入力されるアクセスチケットが有効か否かを検証することを特徴とする請求項１または２記載の情報アクセス制御方法。

【請求項７】　前記アクセス要求を許可するか否かを判定する処理は、アクセスチケットの各状態に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを特徴とする請求項１記載の情報アクセス制御方法。

【請求項８】　前記アクセス要求を許可するか否かを判定する処理は、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを特徴とする請求項２記載の情報アクセス制御方法。

【請求項９】　保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御装置であって、

複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行するアクセスチケット発行手段と、

アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定するアクセス権限判定手段と、

アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する状態更新手段とを有することを特徴とする情報アクセス制御装置。

【請求項１０】　保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御装置であって、

アクセスの内容に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行するアクセスチケット発行手段と、
アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定するアクセス権限判定手段と、
アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する状態更新手段とを有することを特徴とする情報アクセス制御装置。

【請求項１１】　前記状態更新手段は、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して格納している状態遷移情報格納手段と、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納手段から読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する手段とを有することを特徴とする請求項９記載の情報アクセス制御装置。

【請求項１２】　前記状態更新手段は、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して格納している状態遷移情報格納手段と、アクセス者から前記状態遷移要求とともに入力されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納手段から読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する手段とを有することを特徴とする請求項１０記載の情報アクセス制御装置。

【請求項１３】　前記状態更新手段は、アクセス者からの前記状態遷移要求に含まれている状態遷移イベントも考慮して前記遷移先状態を決定する手段を有することを特徴とする請求項９乃至１２のいずれかに記載の情報アクセス制御装置。

【請求項１４】　前記要求とともに入力されるアクセスチケットが有効か否かを検証するアクセスチケット検証手段を有することを特徴とする請求項９または１０記載の情報アクセス制御装置。

【請求項１５】　前記アクセス権限判定手段は、アクセスチケットの各状態に対応して規定されるアクセス権限を格納しているアクセスチケット権限情報格納手段と、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納手段から読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する手段とを有することを特徴とする請求項９記載の情報アクセス制御装置。

【請求項１６】　前記アクセス権限判定手段は、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限を格納しているアクセスチケット権限情報格納手段と、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納手段から読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する手段とを有することを特徴とする請求項１０記載の情報アクセス制御装置。

【請求項１７】　保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御プログラムを記録した記録媒体であって、
複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、
アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、
アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを特徴とする情報アクセス制御プログラムを記録した記録媒体。

【請求項１８】　保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御プログラムを記録した記録媒体であって、
アクセスの内容に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、
アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、
アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを特徴とする情報アクセス制御プログラムを記録した記録媒体。

【請求項１９】　前記アクセスチケットの状態を更新する処理は、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して状態遷移情報格納テーブルに格納しておき、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新することを特徴とする請求項１７記載の情報アクセス

制御プログラムを記録した記録媒体。

【請求項２０】　前記アクセスチケットの状態を更新する処理は、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して状態遷移情報格納テーブルに格納しておき、アクセス者から前記状態遷移要求とともに入力されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新することを特徴とする請求項１８記載の情報アクセス制御プログラムを記録した記録媒体。

【請求項２１】　前記アクセスチケットの状態を更新する処理は、アクセス者からの前記状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して前記遷移先状態を決定していることを特徴とする請求項１７乃至２０のいずれかに記載の情報アクセス制御プログラムを記録した記録媒体。

【請求項２２】　前記要求とともに入力されるアクセスチケットが有効か否かを検証することを特徴とする請求項１７または１８記載の情報アクセス制御プログラムを記録した記録媒体。

【請求項２３】　前記アクセス要求を許可するか否かを判定する処理は、アクセスチケットの各状態に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを特徴とする請求項１７記載の情報アクセス制御プログラムを記録した記録媒体。

【請求項２４】　前記アクセス要求を許可するか否かを判定する処理は、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを特徴とする請求項１８記載の情報アクセス制御プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御方法および装置に関し、更に詳しくは、インターネットのような不特定多数のユーザが参加する開放型分散システムにおいてあるユーザが自身の管理する保護対象資源であるターゲット情報に対する他のユーザであるアクセス者によるアクセスを制御すべく制御する情報アクセス制御方法および装置と情報アクセス制御プログラムを記録した記録媒体に関する。特に、本発明は、インターネット上での商取引のようにアクセス者それぞれの目的や役割が取引の局面に応じて変化するために同一のアクセス者に対しても取引の局面の変化に応じて許容するアクセス権限を違える必要があるといった特徴を持つシステムにおける保護対象資源へのアクセスを制御する情報アクセス制御方法および装置と情報アクセス制御プログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】一般に、保護対象資源（ターゲット情報）に対するアクセス制御は、アクセスを試みる主体（アクセス者）と、アクセスされる保護対象資源、ターゲット情報に対するアクセスの種別のセットで記述されたアクセス権限情報に基づいて実施される。アクセス権限情報に基づくアクセス制御の方法として、アクセス制御リスト（ＡＣＬ）に基づくアクセス制御の方法と、アクセス資格（ケイパビリティ）に基づく方法とがある。

【０００３】前者は、個々のターゲット情報毎に、そのターゲット情報に対するアクセスが許容されるアクセス者およびそのアクセスの種別を対にして並べた一覧（ＡＣＬ）に基づいて制御する方法であり、アクセス要求が発生する毎にＡＣＬを探索し、そのアクセス要求を許可するか否かを決定する。これを拡張した方法として、ロールに基づくアクセス制御の方法がある。この方法では、複数のアクセス者に同一のアクセス権限が許容する場合に、それらアクセス者をロールと呼ばれる単位にまとめ、各ロールに対するアクセス権限を記述・管理する。

【０００４】一方、後者は、あるターゲット情報に対するある種別のアクセスを行うアクセス権限を表すデータ（ケイパビリティ）を用いて制御する方法であり、アクセス要求の内容を含むアクセス権限を表すケイパビリティがアクセス者から提示された場合に、そのアクセス要求を許可する。ケイパビリティの無効リストなどを用いて、発行済みケイパビリティの無効／有効を制御することも可能である。このケイパビリティに基づく方法では、アクセス要求が発生する毎に、ＡＣＬを探索する必要はない。

【０００５】

【発明が解決しようとする課題】誰でもが自由に参加できるインターネット上での商取引のように、不特定多数のアクセス者が想定され、またアクセス者それぞれの目的や役割が取引の局面に応じて変化するために、同一のアクセス者に対しても、取引の局面の変化に応じて、許容するアクセス権限を違える必要があるといった特徴を持つ環境においては、上述した従来のアクセス制御の方法では、以下のような問題が生ずる。

【０００６】まず、ＡＣＬあるいはロールに基づくアクセス制御の方法では、アクセス者へのアクセス権限の割り当て、あるいは、アクセス者へのロールの割り当ておよびロールへのアクセス権限の割り当ては固定的なものであり、同一のアクセス者に許容するアクセス権限を取引の局面の変化に応じて変更することはできない。

【０００７】また、ケイパビリティに基づくアクセス制御の方法では、同じアクセス者に対しても、取引の局面が変化する度に、新しい局面に応じたケイパビリティを発行・付与したり、また発行・付与済みのケイパビリティを無効化したりする必要がある。

【０００８】このため、アクセス制御側でのケイパビリティ発行数の増加による発行・付与処理コストの増加、および発行済みケイパビリティの制御・管理の煩雑化、およびアクセス者側での、保有しなければならないケイパビリティ数の増加によるケイパビリティの管理コストおよび適切なケイパビリティを使い分けるための処理コストの増加といった問題が生じる。

【０００９】本発明は、上記に鑑みてなされたもので、その目的とするところは、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更することができる情報アクセス制御方法および装置と情報アクセス制御プログラムを記録した記録媒体を提供することにある。

【００１０】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御方法であって、複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを要旨とする。

【００１１】請求項１記載の本発明にあっては、各状態毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この遷移先状態でアクセスチケットの状態を更新するため、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更でき、柔軟なアクセス制御を実現することができる。

【００１２】また、請求項２記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御方法であって、アクセスの内容に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを要旨とする。

【００１３】請求項２記載の本発明にあっては、複数の種類の複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求を受け付けた場合、アクセスチケットの種類および状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、また状態遷移要求を受け付けた場合、アクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新するため、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更でき、柔軟なアクセス制御を実現することができる。

【００１４】更に、請求項３記載の本発明は、請求項１記載の発明において、前記アクセスチケットの状態を更新する処理が、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して状態遷移情報格納テーブルに格納しておき、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新することを要旨とする。

【００１５】請求項３記載の本発明にあっては、アクセスチケットの各状態の遷移先状態を状態遷移情報格納テーブルに格納しておき、アクセス者からの状態遷移要求の入力時、状態遷移情報格納テーブルからアクセスチケットの状態に対応する遷移先状態を読み出し、この遷移先状態でアクセスチケットの状態を更新する。

【００１６】請求項４記載の本発明は、請求項２記載の発明において、前記アクセスチケットの状態を更新する処理が、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して状態遷移情報格納テーブルに格納しておき、アクセス者から前記状態遷移要求とともに入力

されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新することを要旨とする。

【００１７】請求項４記載の本発明にあっては、各種類のアクセスチケットの各状態の遷移先状態を状態遷移情報格納テーブルに格納しておき、アクセス者から状態遷移要求の入力時、アクセスチケットの種類および状態に対応する遷移先状態を状態遷移情報格納テーブルから読み出し、この遷移先状態でアクセスチケットの状態を更新する。

【００１８】また、請求項５記載の本発明は、請求項１乃至４のいずれかに記載の発明において、前記アクセスチケットの状態を更新する処理が、アクセス者からの前記状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して前記遷移先状態を決定していることを要旨とする。

【００１９】請求項５記載の本発明にあっては、アクセス者からの状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して遷移先状態を決定している。

【００２０】更に、請求項６記載の本発明は、請求項１または２記載の発明において、前記要求とともに入力されるアクセスチケットが有効か否かを検証することを要旨とする。

【００２１】請求項６記載の本発明にあっては、状態遷移要求やアクセス要求等の要求とともに入力されるアクセスチケットが有効か否かを検証している。

【００２２】請求項７記載の本発明は、請求項１記載の発明において、前記アクセス要求を許可するか否かを判定する処理が、アクセスチケットの各状態に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを要旨とする。

【００２３】請求項７記載の本発明にあっては、アクセスチケットの各状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、アクセス要求時、アクセスチケットの状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルから読み出し、このアクセス権限に基づいてアクセス要求を許容するか否かを判定している。

【００２４】また、請求項８記載の本発明は、請求項２または４記載の発明において、前記アクセス要求を許可するか否かを判定する処理が、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを要旨とする。

【００２５】請求項８記載の本発明にあっては、アクセスチケットの複数の種類の複数の状態の各々に対応するアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、アクセス要求時、アクセスチケットの種類および状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルから読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定している。

【００２６】更に、請求項９記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御装置であって、複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行するアクセスチケット発行手段と、アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定するアクセス権限判定手段と、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する状態更新手段とを有することを要旨とする。

【００２７】請求項９記載の本発明にあっては、各状態毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この遷移先状態でアクセスチケットの状態を更新するため、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更でき、柔軟なアクセス制御を実現することができる。

【００２８】請求項１０記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御装置であって、アクセスの内容に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行するアクセスチケット発行手段と、アクセス者からのアクセス要求を受け付け、この要求とともに入力され

たアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定するアクセス権限判定手段と、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する状態更新手段とを有することを要旨とする。

【００２９】請求項１０記載の本発明にあっては、複数の種類の複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求を受け付けた場合、アクセスチケットの種類および状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、また状態遷移要求を受け付けた場合、アクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新するため、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更でき、柔軟なアクセス制御を実現することができる。

【００３０】また、請求項１１記載の本発明は、請求項９記載の発明において、前記状態更新手段が、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して格納している状態遷移情報格納手段と、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納手段から読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する手段とを有することを要旨とする。

【００３１】請求項１１記載の本発明にあっては、アクセスチケットの各状態の遷移先状態を状態遷移情報格納手段に格納しておき、アクセス者からの状態遷移要求の入力時、状態遷移情報格納手段からアクセスチケットの状態に対応する遷移先状態を読み出し、この遷移先状態でアクセスチケットの状態を更新する。

【００３２】更に、請求項１２記載の本発明は、請求項１０記載の発明において、前記状態更新手段が、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して格納している状態遷移情報格納手段と、アクセス者から前記状態遷移要求とともに入力されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納手段から読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する手段とを有することを要旨とする。

【００３３】請求項１２記載の本発明にあっては、各種類のアクセスチケットの各状態の遷移先状態を状態遷移情報格納手段に格納しておき、アクセス者から状態遷移要求の入力時、アクセスチケットの種類および状態に対応する遷移先状態を状態遷移情報格納手段から読み出し、この遷移先状態でアクセスチケットの状態を更新する。

【００３４】請求項１３記載の本発明は、請求項９乃至１２のいずれかに記載の発明において、前記状態更新手段が、アクセス者からの前記状態遷移要求に含まれている状態遷移イベントも考慮して前記遷移先状態を決定する手段を有することを要旨とする。

【００３５】請求項１３記載の本発明にあっては、アクセス者からの状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して遷移先状態を決定している。

【００３６】また、請求項１４記載の本発明は、請求項９または１０記載の発明において、前記要求とともに入力されるアクセスチケットが有効か否かを検証するアクセスチケット検証手段を有することを要旨とする。

【００３７】請求項１４記載の本発明にあっては、状態遷移要求やアクセス要求等の要求とともに入力されるアクセスチケットが有効か否かを検証している。

【００３８】更に、請求項１５記載の本発明は、請求項９記載の発明において、前記アクセス権限判定手段が、アクセスチケットの各状態に対応して規定されるアクセス権限を格納しているアクセスチケット権限情報格納手段と、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納手段から読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する手段とを有することを要旨とする。

【００３９】請求項１５記載の本発明にあっては、アクセスチケットの各状態に対応するアクセス権限をアクセスチケット権限情報格納手段に格納しておき、アクセス要求時、アクセスチケットの状態に対応するアクセス権限をアクセスチケット権限情報格納手段から読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定している。

【００４０】請求項１６記載の本発明は、請求項１０記載の発明において、前記アクセス権限判定手段が、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限を格納しているアクセスチケット権限情報格納手段と、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納手段から読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する手段とを有することを要旨とする。

【００４１】請求項１６記載の本発明にあっては、アクセスチケットの複数の種類の複数の状態の各々に対応するアクセス権限をアクセスチケット権限情報格納手段に格納しておき、アクセス要求時、アクセスチケットの種類および状態に対応するアクセス権限をアクセスチケッ

ト権限情報格納手段から読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定している。

【００４２】また、請求項１７記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御プログラムを記録した記録媒体であって、複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【００４３】請求項１７記載の本発明にあっては、各状態毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００４４】更に、請求項１８記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御プログラムを記録した記録媒体であって、アクセスの内容に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【００４５】請求項１８記載の本発明にあっては、複数の種類の複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求を受け付けた場合、アクセスチケットの種類および状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、また状態遷移要求を受け付けた場合、アクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００４６】請求項１９記載の本発明は、請求項１７記載の発明において、前記アクセスチケットの状態を更新する処理が、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して状態遷移情報格納テーブルに格納しておき、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【００４７】請求項１９記載の本発明にあっては、アクセスチケットの各状態の遷移先状態を状態遷移情報格納テーブルに格納しておき、アクセス者からの状態遷移要求の入力時、状態遷移情報格納テーブルからアクセスチケットの状態に対応する遷移先状態を読み出し、この遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００４８】また、請求項２０記載の本発明は、請求項１８記載の発明において、前記アクセスチケットの状態を更新する処理が、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して状態遷移情報格納テーブルに格納しておき、アクセス者から前記状態遷移要求とともに入力されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【００４９】請求項２０記載の本発明にあっては、各種類のアクセスチケットの各状態の遷移先状態を状態遷移情報格納テーブルに格納しておき、アクセス者から状態遷移要求の入力時、アクセスチケットの種類および状態に対応する遷移先状態を状態遷移情報格納テーブルから読み出し、この遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００５０】更に、請求項２１記載の本発明は、請求項１７乃至２０のいずれかに記載の発明において、前記アクセスチケットの状態を更新する処理が、アクセス者か

らの前記状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して前記遷移先状態を決定している情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【００５１】請求項２１記載の本発明にあっては、アクセス者からの状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して遷移先状態を決定している情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００５２】請求項２２記載の本発明は、請求項１７または１８記載の発明において、前記要求とともに入力されるアクセスチケットが有効か否かを検証する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【００５３】請求項２２記載の本発明にあっては、状態遷移要求やアクセス要求等の要求とともに入力されるアクセスチケットが有効か否かを検証している情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００５４】また、請求項２３記載の本発明は、請求項１７記載の発明において、前記アクセス要求を許可するか否かを判定する処理が、アクセスチケットの各状態に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【００５５】請求項２３記載の本発明にあっては、アクセスチケットの各状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、アクセス要求時、アクセスチケットの状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルから読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定している情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００５６】更に、請求項２４記載の本発明は、請求項１８記載の発明において、前記アクセス要求を許可するか否かを判定する処理が、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【００５７】請求項２４記載の本発明にあっては、アクセスチケットの複数の種類の複数の状態の各々に対応するアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、アクセス要求時、アクセスチケットの種類および状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルから読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定している情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００５８】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図１は、本発明の一実施形態に係る情報アクセス制御方法を実施する情報アクセス制御装置の構造を示すブロック図である。

【００５９】なお、本実施形態では、それぞれネットワークに接続されたユーザＡの端末とユーザＢの端末の間において、ユーザＢの端末に格納されているユーザＢ所有の情報（ターゲット情報）への、ユーザＡによるアクセスをユーザＢの端末に設けた本発明によるアクセス制御システムによってアクセス制御する場合について述べる。

【００６０】また、本実施形態では、ユーザＡと、ユーザＢがネットワーク上の情報伝達手段であるWorld Wide Web（WWW）や電子メイル等を用いて、ネットワーク上で商品の売買を行うという場面を想定し、販売者ユーザＡが、売買取引の進行に応じて、購入者ユーザＢの端末に格納されているユーザＢの住所や氏名などといった情報にアクセスする際のアクセス制御について述べる。

【００６１】図１に示す情報アクセス制御装置について説明する。図１において、１はアクセスチケットを発行するアクセスチケット発行手段であり、２はアクセス要求を許可するかどうか判定するアクセス権限判定手段であり、３はアクセスチケットが有効なものかどうか検証するアクセスチケット検証手段であり、４はアクセスチケットの状態遷移を実施する状態遷移実施手段である。５はアクセスチケットの状態とその遷移の仕方を記述した状態遷移情報１０５を格納する状態遷移情報格納手段であり、６はアクセスチケットの各状態に対応するアクセス権限を記述したアクセスチケット権限情報１０６を格納するアクセスチケット権限情報格納手段であり、７は有効なアクセスチケットに関する情報である有効アクセスチケット情報１０７を格納する有効アクセスチケット情報格納手段であり、８はターゲット情報１０８を格納するターゲット情報格納手段である。

【００６２】また、９はアクセス制御システムを備えたユーザＢの対話型端末であり、１０はＤＥＳ（Data Encryption Standard）などの対称型暗号方式による共通鍵

であってアクセスチケットの生成および検証に用いられるアクセスチケット生成検証鍵ｋ１１０を格納するアクセスチケット生成検証鍵格納手段であり、１１はアクセスチケットの生成および検証に補助的に用いられるアクセスチケット生成検証補助データｄ１１１を格納するアクセスチケット生成検証補助データ格納手段であり、１２はターゲット情報１０８に対してアクセスを行うアクセス者ユーザＡの端末であり、１３はターゲット情報所有者の端末９およびアクセス者の端末１２などを結ぶ通信ネットワークであり、１４は本発明によるアクセス制御の処理手順が記述されたプログラムであり、１５はプログラム１４に基づき処理を行う機能を有するＣＰＵである。

【００６３】また、図２は、図１の有効アクセスチケット情報格納手段７に格納された有効アクセスチケット情報１０７のある時点での登録内容を示しており、有効なアクセスチケットそれぞれについて、アクセスチケットを一意に識別するアクセスチケットＩＤと、アクセスチケット種別と、その時点における状態を保持している。

【００６４】図３は、図１の状態遷移情報格納手段５に格納された状態遷移情報１０５の内容を示しており、アクセスチケットの種別毎に、取り得る状態３１１、初期状態３１２、状態遷移規則３１３、最終状態３１４が記述される。また、各状態遷移規則は遷移元状態３２１、状態遷移イベント名称３２２、遷移先状態３２３から構成される。

【００６５】図４は、図１のアクセスチケット権限情報格納手段６に格納されたアクセスチケット権限情報１０６の内容を示しており、アクセスチケットの種別毎に、取り得る状態それぞれに対応するアクセス権限が記述される。また、各アクセス権限は、ターゲット情報の識別子とそれに対するアクセス種別の組で構成される。

【００６６】図５は、図１のターゲット情報格納手段８に格納されたターゲット情報１０８の内容を示しており、階層化された項目５０１と、それぞれの項目に対応する情報（値）５０２とで構成される。

【００６７】次に、上述したように構成される本実施形態の情報アクセス制御装置の作用を説明する。なお、この説明では、アクセスチケット情報の所有者であるユーザＢは予めアクセスチケットの種別毎にその状態遷移情報１０５およびアクセスチケット権限情報１０６を記述し、それぞれ状態遷移情報格納手段５およびアクセスチケット権限情報格納手段６に格納しているものとする。また、状態遷移情報１０５およびアクセスチケット権限情報１０６はそれぞれ図３、図４に示すように定義されているものとする。

【００６８】まず、アクセスチケットの発行について図６に示すフローチャートを参照して説明する。

【００６９】本実施形態では、ターゲット情報所有者のユーザＢは、アクセス者のユーザＡによるアクセスに先だって、ユーザＡに許容すべき適切なアクセス権限と対応するアクセスチケットを与えるため、適切なアクセスチケットの種別を指定して、アクセス制御システムにアクセスチケットの生成を命じる。

【００７０】これは例えば、ユーザＢがユーザＡの開設するＷＷＷ上の仮想的な商店であるホームページ（電子ショップ）を訪れた時点などで行われる。

【００７１】本発明によれば、アクセスチケットの生成を指示されたアクセス制御システムはアクセスチケット発行手段１を用いて、指定された種別を持つアクセスチケットを新規に生成し、出力する。

【００７２】図６に示すアクセスチケット発行手続きでは、まず、ステップＳ６０２で、指定されたアクセスチケットの種別ｔｙｐｅ１を取得し、ステップＳ６０３で新しくユニークなアクセスチケットＩＤｉｄ１を払い出す。

【００７３】ここで、アクセスチケットＩＤの生成・払出の方法としては、アクセスチケットＩＤの検索を容易にするため、またアクセスチケットＩＤを格納する領域が小さくて済むように、アクセスチケットＩＤのデータサイズが可能な限り小さいものであるようにする必要がある。このため、本実施形態では、ステップＳ６０３におけるアクセスチケットＩＤの生成・払出の方法として、０（ゼロ）から連続した整数値を払い出す方法を採用している。

【００７４】そして、ステップＳ６０４、ステップＳ６０５で、アクセスチケット生成検証補助データｄ１１１と、アクセスチケット生成検証鍵ｋ１１０とを取得し、ステップＳ６０６で（アクセスチケットＩＤｉｄ１、アクセスチケット生成検索補助データｄ１１１）なる形式のデータを鍵ｋ１１０で暗号化し、これを新規アクセスチケットｔ１とする。

【００７５】その後、ステップＳ６０７で、状態遷移情報１０５から、アクセスチケット種別ｔｙｐｅ１に対応する状態遷移情報ｓｉ１を取得し、ステップＳ６０８で、ｓｉ１から初期状態ｓ１を取得する。

【００７６】そして、ステップＳ６０９で、アクセスチケット種別ｔｙｐｅ１と、初期状態ｓ１とともに、アクセスチケットＩＤｉｄ１を、有効アクセスチケット情報１０７に登録した後、ステップＳ６１０で、同アクセスチケットｔ１を出力する。出力されたアクセスチケットの構造を図１３に示す。

【００７７】ここで、状態遷移情報１０５が図３に示す状態であり、また、生成するアクセスチケットの種別として、“購入取引１”が指定され、また、ステップＳ６０３においては新規アクセスチケットＩＤとして、０００１が払い出されるとすると、上記手順により、図３に示す状態遷移情報１０５の内容に基づいて、“購入取引１”を種別とし、“閲覧中”をその状態とするアクセスチケットｔ２が生成され、その情報が有効アクセス

チケット情報１０７に登録される。

【００７８】ここで、ｔ２は、払い出されたアクセスチケットＩＤ０００４と、アクセスチケット生成検証補助データｄ１１１を（アクセスチケットＩＤ０００４、アクセスチケット生成検証補助データｄ１１１）の形式にしたものをアクセスチケット生成検証鍵ｋ１１０で暗号化したものである。

【００７９】同アクセスチケットｔ２が有効アクセスチケット情報１０７に登録された様子を図１２に示す。

【００８０】このようにして、アクセスチケットｔ２が発行されると、ユーザＢは、ＳＳＬ（Secure Socket Layer）などによりユーザＡとの間で安全な通信路を確立した上で、同アクセスチケットを送信する。

【００８１】次に、アクセス要求処理、アクセスチケット検証処理、アクセス権限判定処理について図８、図９、図１０のフローチャートを参照して説明する。

【００８２】本実施形態では、アクセス者であるユーザＡは、ユーザＢの情報（ターゲット情報）にアクセスする際に、そのアクセスの内容を示すアクセス要求と、先にユーザＢから取得していたアクセスチケットとを安全な通信路を介してアクセス制御システムに送信する。

【００８３】アクセス制御システムにおけるアクセス要求処理手続きを図８を用いて詳細に説明する。

【００８４】まず、ステップＳ８０２、ステップＳ８０３で、受信したアクセス要求ｒｅｑ１とアクセスチケットｔ１とをそれぞれ取得する。そして、ステップＳ８０４で、アクセスチケットｔ１が有効かどうかをアクセスチケット検証手段３を用いて判定する。

【００８５】このアクセスチケット検証手続きを図７を用いてより詳細に説明する。

【００８６】まず、ステップＳ７０２で、アクセスチケットｔ１を取得し、ステップＳ７０３でアクセスチケット生成検証鍵ｋ１１０を取得する。次いで、ステップＳ７０４で、ｔ１に対してｋ１１０による復号化を試み、失敗した場合には、同アクセスチケットｔ１を無効と判定する（ステップＳ７０９）。

【００８７】復号できた場合は、その結果得られたデータをｍ１とし（ステップＳ７０５）、ステップＳ７０６でアクセスチケット生成検証補助データｄ１１１を取得し、ステップＳ７０７で、ｍ１＝（アクセスチケットＩＤｉｄ１、アクセスチケット生成検証補助データｄ１１１）なるアクセスチケットＩＤが有効アクセスチケット情報１０７に登録されているか確認する。登録されていなければ、アクセスチケットｔ１を無効と判定する（ステップＳ７０９）。登録されていれば、同アクセスチケットＩＤｉｄ１をアクセスチケットｔ１のアクセスチケットＩＤとして一時的に（アクセス要求処理手続きが終わるまでの間）保存し、アクセスチケットｔ１を有効と判定する（ステップＳ７０８）。

【００８８】上記アクセスチケット検証手続きによってアクセスチケットｔ１が無効と判定された場合、アクセス制御システムは、アクセス要求ｒｅｑ１を拒否し、これに対する処理を終了する。有効と判定された場合には、アクセス要求ｒｅｑ１を拒否するか否かをアクセス権限判定手段２を用いて判定する（ステップＳ８０５）。

【００８９】この手続きを図９を用いてより詳細に説明する。

【００９０】まず、ステップＳ９０２、ステップＳ９０３で、アクセス要求ｒｅｑ１とアクセスチケットｔ１をそれぞれ取得し、ステップＳ９０４で、有効アクセスチケット情報１０７から、アクセスチケットｔ１に対応するアクセスチケット種別ｔｙｐｅ１と、その時点におけるアクセスチケットｔ１の状態ｓ１を取得し、ステップＳ９０５で、アクセスチケット権限情報１０６から種別ｔｙｐｅ１に対応するアクセスチケット権限情報ｒｉ１を取得し、ステップＳ９０６で、アクセスチケット権限情報ｒｉ１から、アクセスチケットｔ１の状態ｓ１に対応するアクセス権限Ｒ１を取得し、これを、その時点で、アクセスチケットｔ１に対応するアクセス権限と決定する。

【００９１】そして、ステップＳ９０７で、アクセス権限Ｒ１が、アクセス要求ｒｅｑ１で示されるアクセス内容を含むかどうかを検査する。含まれない場合、アクセス権限Ｒ１は、アクセス要求ｒｅｑ１に対して無効であり、同アクセス要求ｒｅｑ１を不許可とする（ステップＳ９０９）。含まれていれば、許可と判定する（ステップＳ９０８）。

【００９２】アクセス権限判定手段２によってアクセス要求ｒｅｑ１が不許可と判定された場合、アクセス制御システムは、同アクセス要求ｒｅｑ１を拒否し、これに対する処理を終了する。有効と判定された場合には、ステップＳ８０６で、アクセス要求ｒｅｑ１の内容を処理し、その返答をユーザＡに安全な通信路を介して送信する。

【００９３】ここで、本実施形態においては、ユーザＡが、ユーザＢの端末９のアクセス制御システムに対して、「年齢の参照」というアクセス要求ｒｅｑ２を、予め取得してあったアクセスチケットｔ２とともに送信したとする。

【００９４】また、この時の有効アクセスチケット情報１０７の登録内容は、図１２に示す通りであり、アクセスチケット権限情報１０６の内容は、図４に示す通りであるとする。

【００９５】まず、アクセス制御システムは、アクセス要求ｒｅｑ２（＝「年齢：参照」）とアクセスチケットｔ２とを取得し（ステップＳ８０２、ステップＳ８０３）、アクセスチケットｔ２が有効かどうかを、アクセスチケット検証手段３を用いて判定する（ステップＳ８０４）。

【００９６】アクセスチケット検証手段３では、上述の手順（ステップＳ７０１～ステップＳ７０８）により、アクセスチケットｔ２は、アクセスチケットＩＤ０００４を持つ有効なアクセスチケットと判定される。

【００９７】アクセスチケットｔ２が有効と判定されたので、次に、アクセス権限判定手段２を用いて、アクセス要求ｒｅｑ２を許可するかどうかを判定する（ステップＳ８０５）。

【００９８】アクセス権限判定手段２では、上述の手順の通り、アクセス要求ｒｅｑ２とアクセスチケットｔ２とを取得し（ステップＳ９０２、ステップＳ９０３）、図１２に示す有効アクセスチケット情報１０７の登録内容から、ｔ２の種別“購入取引１”と、状態“閲覧中”を取得する（ステップＳ９０４）。

【００９９】次に、図４に示すアクセスチケット権限情報１０６から、アクセスチケットｔ２の種別“購入取引１”に対応するアクセスチケット権限情報を取得し（ステップＳ９０５）、これから、状態“閲覧中”に対応するアクセス権限（図４の）４０１を取得し、これをアクセスチケットｔ２に対応するアクセス権限として決定する（ステップＳ９０６）。

【０１００】そして、同アクセス権限４０１が、アクセス要求ｒｅｑ２の内容「年齢：参照」を含むことから、アクセス要求ｒｅｑ２に対して有効であることになり、アクセス要求ｒｅｑ２に許可の判定を下す（ステップＳ９０７、ステップＳ９０８）。

【０１０１】アクセス要求ｒｅｑ２が許可と判定されたので、最後にこの内容を処理する。すなわち、ユーザＢの年齢が、ターゲット情報１０８から読み出され、ユーザＡに安全な通信路を介して返信される（ステップＳ８０６）。

【０１０２】次に、状態遷移について図１０、図１１のフローチャートを参照して説明する。

【０１０３】本実施形態では、アクセス者のユーザＡ、もしくは、ターゲット情報所有者のユーザＢは、両者の取引の局面が変化するとともに、ユーザＡに付与されているアクセスチケットの状態を更新し、対応するアクセス権限を変更するために、アクセスチケットと状態遷移イベント名称を指定した状態遷移要求をアクセス制御システムに安全な通信路を介して送信する。

【０１０４】アクセス制御システムにおける状態遷移要求処理手続きを図１０を用いて詳細に説明する。

【０１０５】アクセス制御システムは、まずステップＳ１００２、ステップＳ１００３で、受信した状態遷移要求ｓｒｅｑ１から、状態遷移イベント名称ｅ１とアクセスチケットｔ１とをそれぞれ取得する。そして、ステップＳ１００４で、アクセスチケットｔ１が有効かどうかを、アクセスチケット検証手段３を用いて判定する。この手続きは、既に説明した通りであるので省略する。

【０１０６】アクセスチケット検証手続きによってアクセスチケットｔ１が無効と判定された場合、アクセス制御システムは、状態遷移要求ｓｒｅｑ１を拒否し、これに対する処理を終了する。有効と判定された場合には、上記イベント名称ｅ１とアクセスチケットｔ１とを状態遷移実施手段４に入力し、状態遷移実施手続きを実行させる（ステップＳ１００５）。

【０１０７】この手続きを図１１を用いてより詳細に説明する。

【０１０８】状態遷移実施手段４では、ステップＳ１１０２、ステップＳ１１０３で、状態遷移イベント名称ｅ１とアクセスチケットｔ１とをそれぞれ取得し、ステップＳ１１０４で、有効アクセスチケット情報１０７より、アクセスチケットｔ１に対応する種別ｔｙｐｅ１と、その時点におけるアクセスチケットｔ１の状態ｓ１を取得し、ステップＳ１１５で、状態遷移情報１０５から、アクセスチケット種別ｔｙｐｅ１に対応する状態遷移情報ｓｉ１を取得する。

【０１０９】次に、ステップＳ１１０６で、状態ｓ１を遷移元状態とし、イベント名称ｅ１を遷移イベントとする状態遷移規則が、状態遷移情報ｓｉ１に存在するか調べる。もし存在しなければ、状態遷移要求ｓｒｅｑ１に対する状態遷移実施手続きを終了する。この場合、アクセスチケットｔ１の状態の変更は一切行われない。

【０１１０】もし上記状態遷移規則が存在すれば、これを状態遷移規則ｒｕｌｅ１として取得する（ステップＳ１１０７）。

【０１１１】そして、ステップＳ１１０８で、有効アクセスチケット情報１０７に保持されているアクセスチケットｔ１の状態を、状態遷移規則ｒｕｌｅ１で指定されている遷移先状態ｓ２に更新する。

【０１１２】更に、ステップＳ１１０９で、アクセスチケットｔ１の遷移後の状態ｓ２が、状態遷移情報ｓｉ１において最終状態として定義されているかどうかを検査する。もし最終状態として定義されていれば、有効アクセスチケット情報１０７からアクセスチケットｔ１に関するすべての項目を削除して上記アクセスチケットを無効化し（ステップＳ１１１０）、状態遷移実施手続きを終了する。ｅ１が最終状態として定義されていなければ、そのまま状態遷移実施手続きを終了する。

【０１１３】ここで、本実施形態においては、ユーザＢが、ユーザＡに対して商品購入の申込を行い、これに合わせて、ユーザＡが、“購入”というイベント名称と、予め取得しておいたアクセスチケットｔ２からなる状態遷移要求ｓｒｅｑ２を、ユーザＢの端末９のアクセス制御システムに送信したとする。

【０１１４】また、この時の有効アクセスチケット情報１０７の内容は図１２に示す通りであり、状態遷移情報１０５の内容は、図３に示す通りであるとする。

【０１１５】まず、アクセス制御システムは、イベント名称“購入”とアクセスチケットｔ２とを取得し（ステ

ップＳ１００２、ステップＳ１００３）、アクセスチケットｔ２が有効かどうかを、アクセスチケット検証手段３を用いて判定する（ステップＳ１００４）。

【０１１６】アクセスチケット検証手段３では、既に述べた手順（ステップＳ７０１～ステップＳ７０８）により、アクセスチケットｔ２は、アクセスチケットＩＤ０００４を持つ有効なアクセスチケットと判定される。

【０１１７】次に、上記イベント名称“購入”とアクセスチケットｔ２とを状態遷移実施手段４に入力し、状態遷移実施手続きを実行させる（ステップＳ１００５）。

【０１１８】状態遷移実施手段４では、上述の手順の通り、イベント名称“購入”とアクセスチケットｔ２とを取得し（ステップＳ１１０２、ステップＳ１１０３）、図１２に示す有効アクセスチケット情報１０７の登録内容から、ｔ２の種別“購入取引１”と、状態“閲覧中”を取得する（ステップＳ１１０４）。

【０１１９】次に、図３に示す状態遷移情報１０５から、アクセスチケットｔ２の種別“購入取引１”に対応する状態遷移情報を読み出し（ステップＳ１１０５）、これから、状態“閲覧中”を遷移元状態とし、イベント“購入”を遷移イベントとする状態遷移規則（図３の）３０１を取得し（ステップＳ１１０６、ステップＳ１１０７）、有効アクセスチケット情報１０７に保持されているアクセスチケットｔ２の状態を、同状態遷移規則３０１で指定されている遷移先状態“注文中”に更新する（ステップＳ１１０８）。

【０１２０】更に、アクセスチケットｔ２の遷移後の状態“注文中”が、最終状態として定義されているかどうか検査する（ステップＳ１１０９）。同状態は、最終状態として定義されていないので、そのまま状態遷移実施手続きを終了する。

【０１２１】この時点におけるアクセスチケットｔ２の状態“注文中”に対応するアクセス権限は、図４に示すアクセスチケット権限情報１０６から、アクセス権限４０２となり、先ほどアクセス要求処理手続きについて述べた際に、アクセスチケットｔ２に対応していたアクセス権限（図４の）４０１とは異なっていることがわかる。

【０１２２】このように、状態遷移要求によってアクセスチケットの状態を変更させることより、同じアクセスチケットに対するアクセス権限を容易に変更することができる。すなわち、同一のアクセス者に対して許容するアクセス権限をアクセスチケットを再発行・再付与することなく、容易に変更することができる。

【０１２３】上述したように、本実施形態では、複数の状態の各々について異なるアクセス権限を対応づけたアクセス権限決定補助データ（アクセスチケット）を発行してアクセス者に付与し、取引上の局面の変化に応じて送付される状態遷移イベントを元に同アクセスチケットの状態を変更することにより、取引上の局面の変化に応じて、同アクセスチケットに対応するアクセス権限、すなわち、同アクセスチケットを保持するアクセス者に対して許容するアクセス権限を変更する。

【０１２４】このため、ケイパビリティを用いた場合には、例えば同一取引の同一アクセス者に対しても局面毎に複数のケイパビリティを発行し付与する必要があったが、本発明によれば、アクセスチケットの発行・付与は一度で済む。よって、これらの発行・付与のコストが大幅に軽減される。

【０１２５】また同様に、ケイパビリティを用いた場合には、局面毎に与えた複数のケイパビリティの有効／無効を制御・管理する必要があったが、本発明によれば、１つのアクセスチケットの状態を制御・管理するので、それらの制御・管理の煩雑さが軽減される。

【０１２６】また同様に、ケイパビリティを用いた場合には、アクセス者は、局面毎に与えられた複数のケイパビリティを保持し、また局面に応じて使い分けなければならなかったが、本発明によれば、アクセス者は１つのアクセスチケットを保持し、これを用いればよいので、それら管理・利用のコストが大幅に軽減される。

【０１２７】上記実施形態において、アクセスチケットの生成方法として、アクセスチケットＩＤに固定のデータ（アクセスチケット生成検証補助データｄ１１１）を組み合わせたデータに対し、秘密の鍵により暗号化を施したものをアクセスチケットとして用いる方法（方法Ａ）を取っているが、これは、以下の点で有利である。

【０１２８】まず、前途の通り、検索の効率や格納領域の節約のために、アクセスチケットＩＤのデータサイズは十分小さい必要があるが、そうした場合、アクセスチケットＩＤをそのままアクセスチケットとする方法（方法Ｂ１）、あるいは、アクセスチケットＩＤに固定のデータを付加してアクセスチケットとする方法（方法Ｂ２）では、あるアクセスチケットＩＤから別のアクセスチケットＩＤが類推される畏が高くなる。すなわち、あるアクセスチケットから、別のアクセスチケットが類推され、偽造される畏が高くなる。

【０１２９】これに対し、本方法Ａでは、アクセスチケットＩＤのデータサイズが小さくとも、十分な長さのアクセスチケット生成検証補助データｄ１１１を付加して暗号化を施せば、あるアクセスチケットから他のアクセスチケットを類推することは困難となる。

【０１３０】また、上記実施形態では、アクセスチケット生成検証鍵ｋ１１０として、対称型暗号方式による共通鍵を用いたが、同アクセスチケット生成検証鍵ｋ１１０の代わりに、ＲＳＡなどの非対称型暗号方式による鍵の鍵対（ペア）を用意し、アクセスチケット生成手続きの際には鍵対の暗号化鍵を、アクセスチケット検証手続きの際には、もう一方の復号化鍵を用いることとして、アクセス制御システムを構成することもできる。

【０１３１】更に、上記実施形態では、アクセスチケッ

ト生成検証鍵ｋ１１０とアクセスチケット生成検証補助データｄ１１１を固定的なデータとしたが、１つのアクセスチケット、あるいはいくつかのアクセスチケットを発行する毎に、これらを新しいものにそれぞれ変更し、アクセスチケット検証時には、同アクセスチケットの発行の際に用いたアクセスチケット生成検証鍵ｋ１１０とアクセスチケット生成検証補助データｄ１１１を取得して用いる方法・構成を取ることも可能である。

【０１３２】この方法によれば、各アクセスチケット、もしくは、いくつかのアクセスチケットの組と、その生成に用いたアクセスチケット生成検証鍵ｋ１１０とアクセスチケット生成検証補助データｄ１１１の組とを対応づける情報を生成・保持する必要があるものの、アクセスチケットの偽造をより困難なものとするため、場合によっては便利である。

【０１３３】また、上記実施形態では、ユーザＡから状態遷移要求が送られたが、状態遷移要求は、ユーザＡ（すなわちアクセス者）、あるいはユーザＢ（すなわちターゲット情報の所有者）のいずれによって送られてもよい。

【０１３４】逆に、状態遷移要求が、ユーザＡ、ユーザＢどちらから送られたものなのかを判定し、それに応じて、状態遷移するか否かを判定することは、アクセス者や、ターゲット情報のアクセス者による不適切な状態遷移要求の送付によるアクセス権限の不正な変更を防止することができるため、便利である。

【０１３５】これは、状態遷移情報１０５内の各状態遷移規則に、イベント元条件という項目を設け、“ターゲット情報所有者”、あるいは、“アクセス者”と記述するようにしておき、状態遷移実施手段４において実行される状態遷移実施手続きのステップＳ１１０８において対象のアクセスチケットｔ１の状態を変更する前に、入力された状態遷移要求ｓｒｅｑ１が、ターゲット情報所有者とアクセス者、いずれから送信されたのかその送信元を識別し、同送信元と状態遷移規則ｒｕｌｃ１のイベント元条件を比較し、一致しなかった場合には、状態遷移要求ｓｒｅｑ１を拒否し、これに対する処理を中止するよう設計・構成することによって実現できる。

【０１３６】また、ユーザＡとユーザＢとの上記取引の状況を監視し、局面の変化が起こった際にそれを自動的に検知し、ユーザＡに付与したアクセスチケットに対する適切な状態遷移要求をアクセス制御システムに送信するソフトウェアプロセスを用いると、より便利である。これは例えば、ユーザＤがユーザＡの電子ショップにアクセスするために用いるWWW閲覧用ソフトウェア（ブラウザ）に組み込まれ、ユーザＢの操作を監視し、その操作に応じて取引の局面の変化を検知し、状態遷移要求を送るようなブラウザの補助ソフトウェアなどを用いることができる。

【０１３７】なお、上述した実施形態の説明において、アクセスチケット等の情報を安全な通信路を介して送信するという記載における安全な通信路とは、第三者による盗聴、改竄などに対する防御措置が取られた通信路であり、既存の任意の暗号技術によって実現される。この通信路としては、例えば、インターネット上の情報流通システムであるWorld Wide Webで普及しているＳＳＬ（Secure Socket Layer）などが用いられる。

【０１３８】

【発明の効果】以上説明したように、本発明によれば、各状態毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求の受付時に、アクセスチケットの状態に対するアクセス権限に基づいてアクセス要求を許可するか否かを判定し、状態遷移要求の受付時、アクセスチケットの状態に基づいて遷移先状態を決定し、この遷移先状態でアクセスチケットの状態を更新するので、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更でき、柔軟なアクセス制御を実現することができる。

【０１３９】また、本発明によれば、複数の種類の複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求の受付時、アクセスチケットの種類および状態に対するアクセス権限に基づいてアクセス要求を許可するか否かを判定し、また状態遷移要求の受付時、アクセスチケットの種類および状態に基づいて遷移先状態を決定し、この遷移先状態でアクセスチケットの状態を更新するので、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更でき、柔軟なアクセス制御を実現することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る情報アクセス制御方法を実施する情報アクセス制御装置の構成を示すブロック図である。

【図２】図１に示す情報アクセス制御装置で使用される有効アクセスチケット情報の登録内容例を示す説明図である。

【図３】図１に示す情報アクセス制御装置で使用されている状態遷移情報格納手段に格納された状態遷移情報の内容を示す説明図である。

【図４】図１に示す情報アクセス制御装置で使用されているアクセスチケット権限情報格納手段に格納されているアクセスチケット権限情報の内容を示す説明図である。

【図５】図１に示す情報アクセス制御装置で使用されているターゲット情報格納手段に格納されているターゲット情報の内容を示す説明図である。

【図６】図１に示す情報アクセス制御装置のアクセスチケット発行手段におけるアクセスチケット発行手続きを示すフローチャートである。

【図７】図１に示す情報アクセス制御装置のアクセスチケット検証手段におけるアクセスチケット検証手続きを示すフローチャートである。

【図８】図１に示す情報アクセス制御装置のアクセス要求処理手続きを示すフローチャートである。

【図９】図１に示す情報アクセス制御装置のアクセス権限判定手段におけるアクセス権限判定手続きを示すフローチャートである。

【図１０】図１に示す情報アクセス制御装置の状態遷移要求処理手続きを示すフローチャートである。

【図１１】図１に示す情報アクセス制御装置の状態遷移実施手段における状態遷移実施手続きを示すフローチャートである。

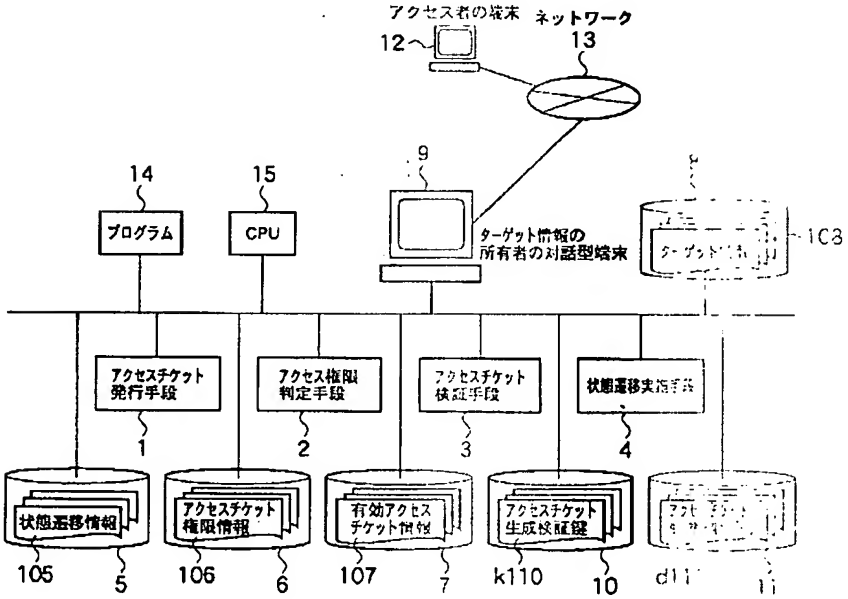
【図１２】図１に示す情報アクセス制御装置で使用される有効アクセスチケット情報の登録内容を示す説明図である。

＊【図１３】図１に示す情報アクセス制御装置におけるアクセスチケット発行手続きにより生成されたアクセスチケットの構造を示す説明図である。

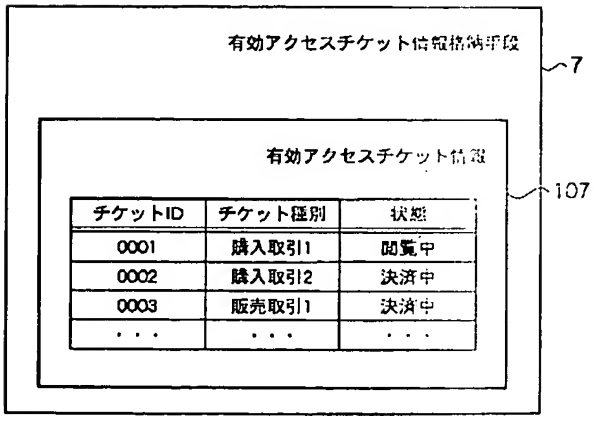
【符号の説明】

1　アクセスチケット発行手段
2　アクセス権限判定手段
3　アクセスチケット検証手段
4　状態遷移実施手段
5　状態遷移情報格納手段
6　アクセスチケット権限情報格納手段
7　有効アクセスチケット情報格納手段
8　ターゲット情報格納手段
9　ターゲット情報所有者の端末
10　アクセスチケット生成検証鍵格納手段
11　アクセスチケット生成検証補助データ格納手段

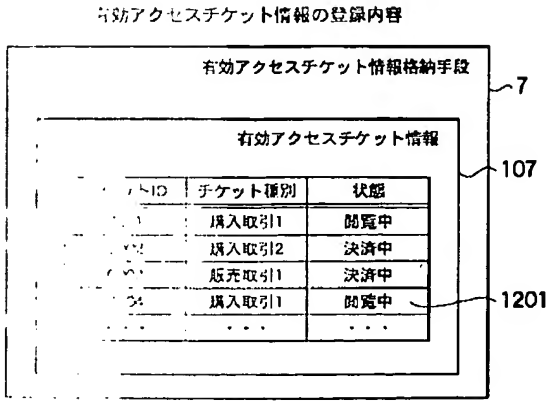
【図１】



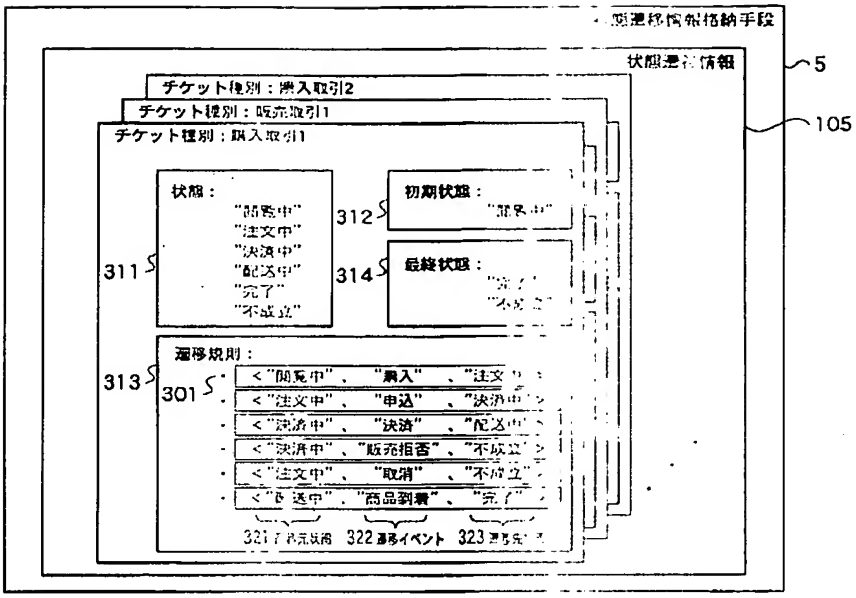
【図２】



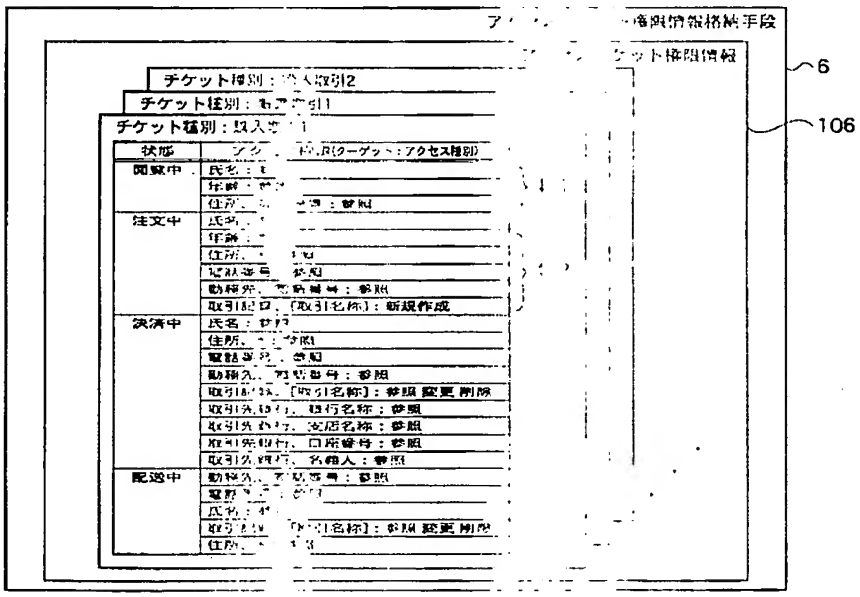
【図１２】



【図３】

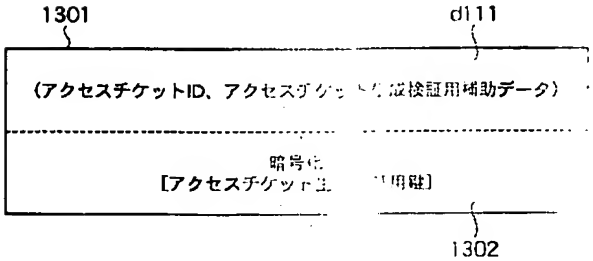


【図４】

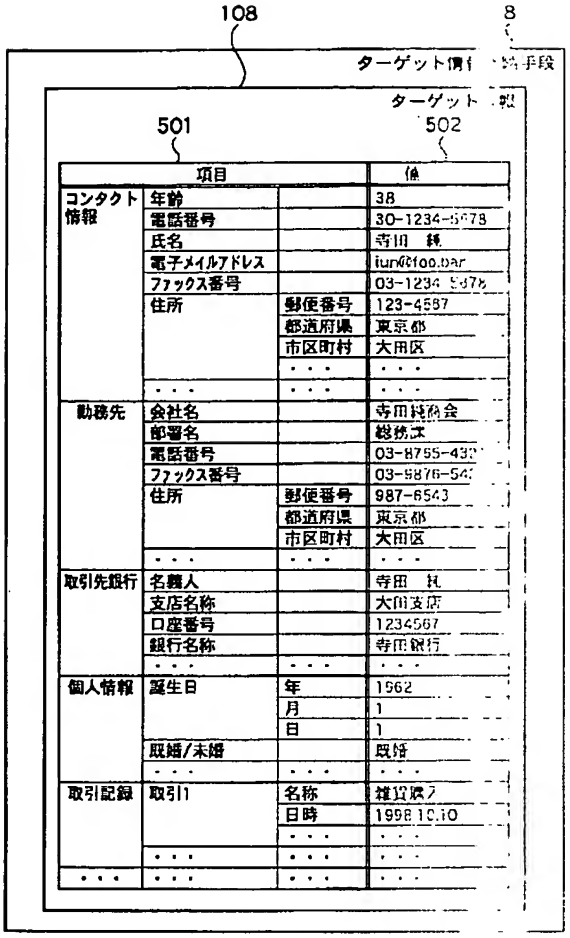


【図１５】

アクセスチケット発行手段により生成された
アクセスチケット

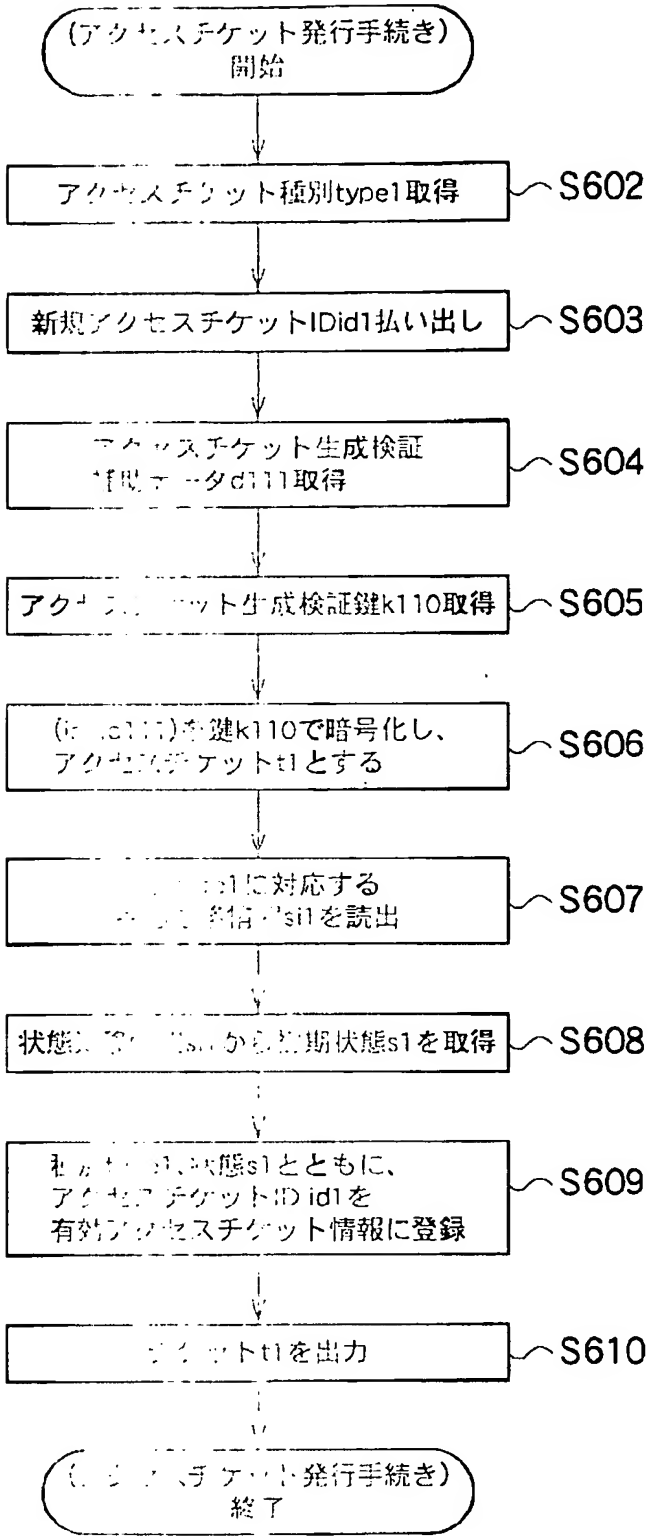


【図5】

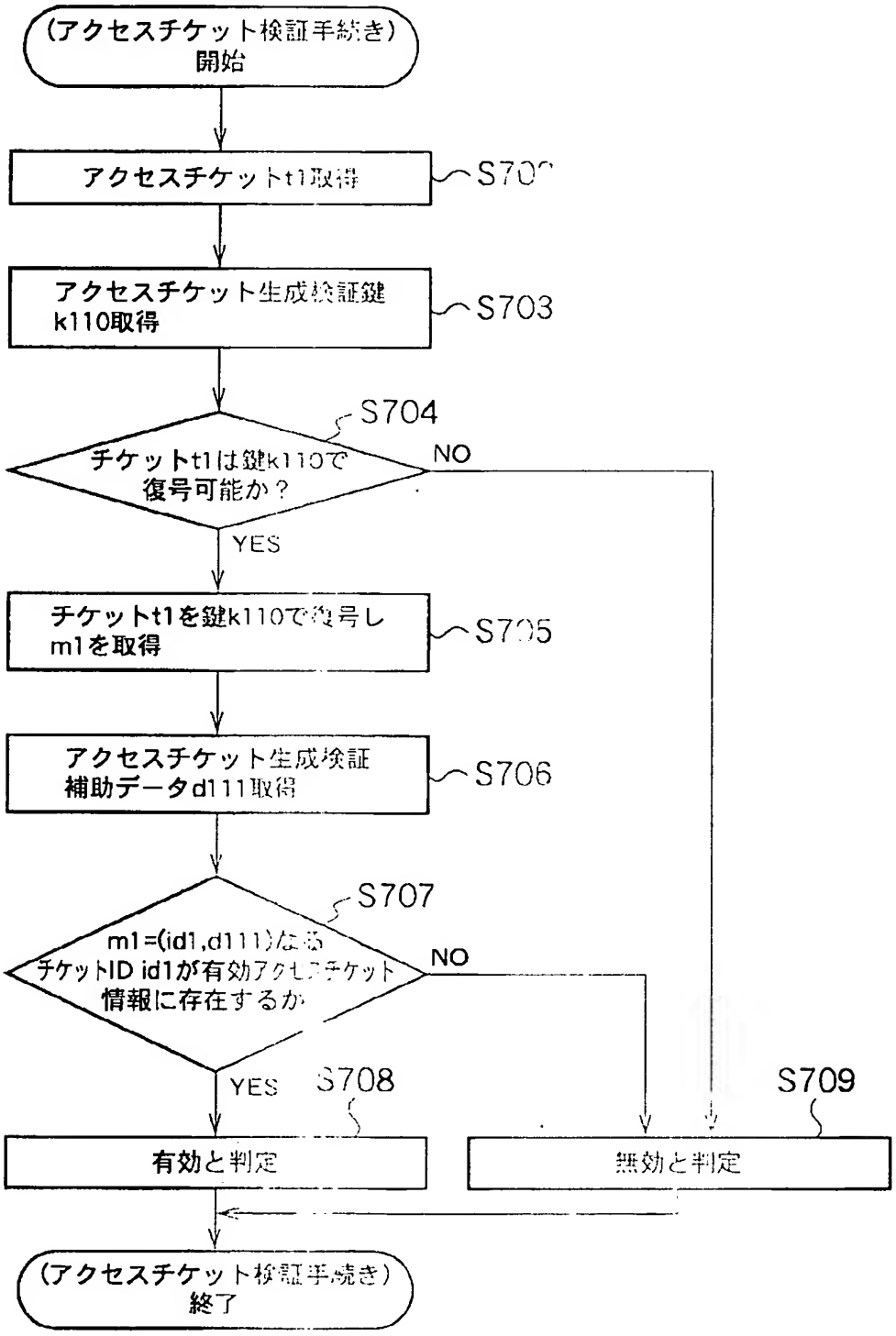


項目			値
コンタクト情報	年齢		38
	電話番号		30-1234-5678
	氏名		寺田　純
	電子メイルアドレス		iun@foo.bar
	ファックス番号		03-1234-5678
	住所	郵便番号	123-4567
		都道府県	東京都
		市区町村	大田区
		・・・	・・・
	・・・	・・・	・・・
勤務先	会社名		寺田純商会
	部署名		総務本
	電話番号		03-8765-43
	ファックス番号		03-5876-54
	住所	郵便番号	987-6543
		都道府県	東京都
		市区町村	大田区
	・・・	・・・	・・・
取引先銀行	名義人		寺田　純
	支店名称		大田支店
	口座番号		1234567
	銀行名称		寺田銀行
	・・・	・・・	・・・
個人情報	誕生日	年	1962
		月	1
		日	1
	既婚/未婚		既婚
	・・・	・・・	・・・
取引記録	取引1	名称	雑貨購入
		日時	1998.10.10
		・・・	・・・
	・・・	・・・	・・・
・・・	・・・	・・・	・・・

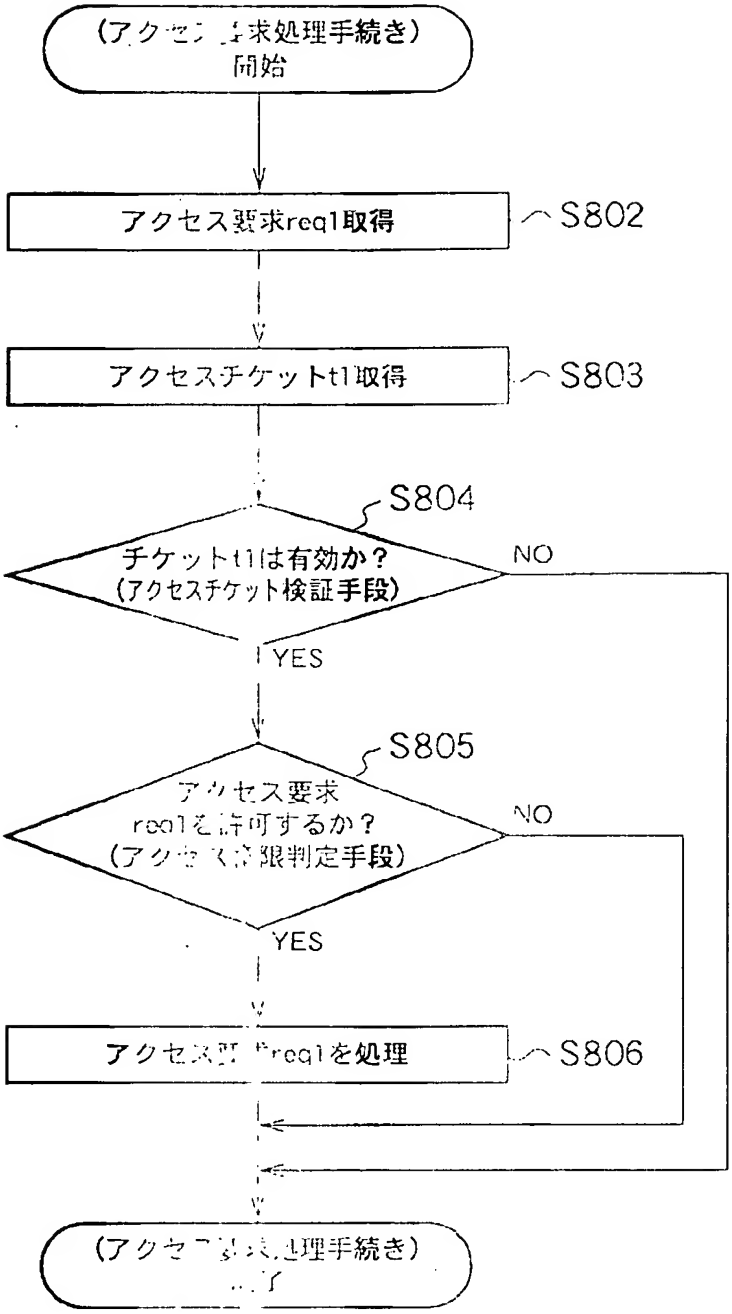
【図6】



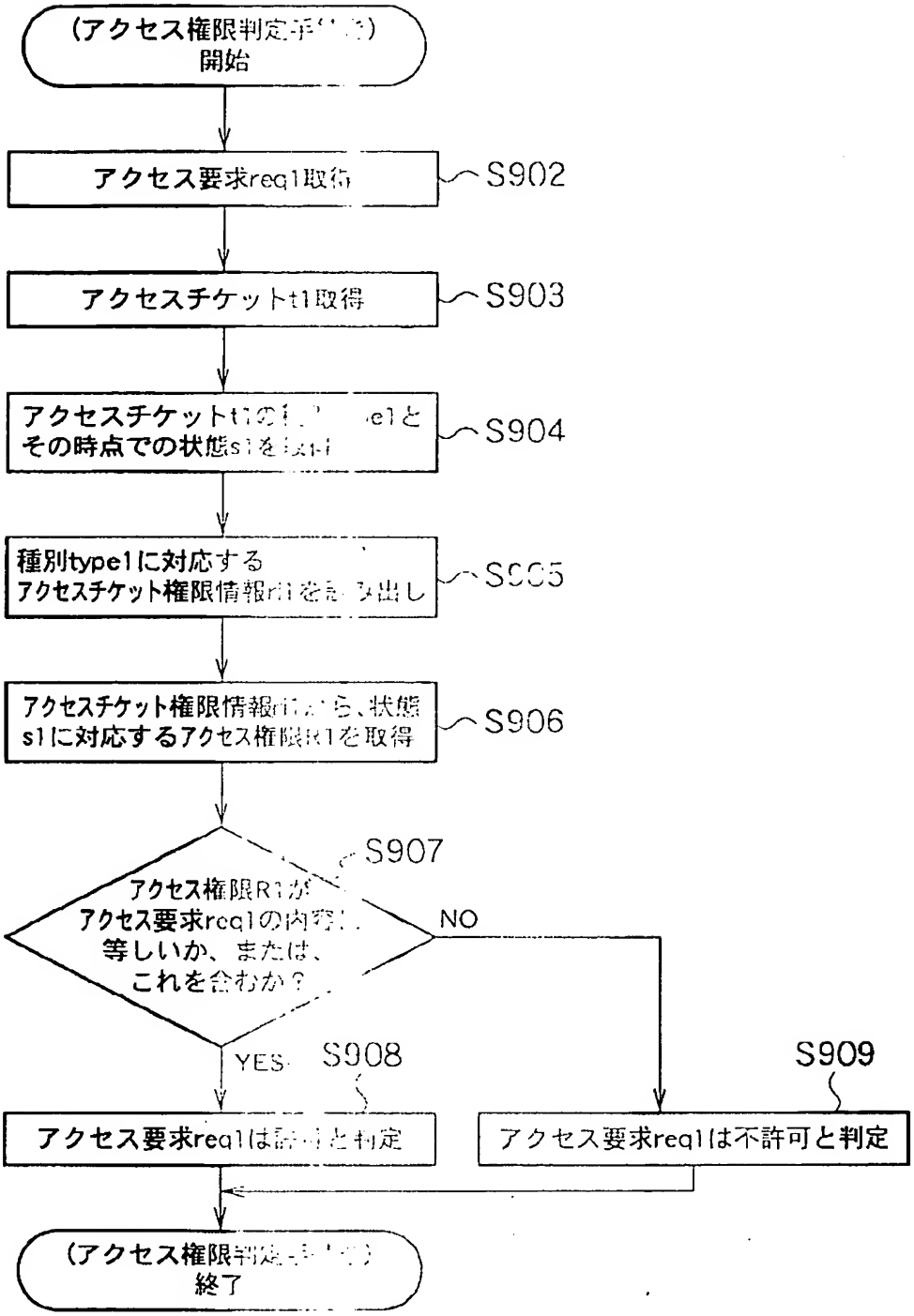
【図7】


(アクセスチケット検証手続き)
開始
アクセスチケットt1取得
S702
アクセスチケット生成検証鍵
k110取得
S703
S704
チケットt1は鍵k110で
復号可能か？
NO
YES
チケットt1を鍵k110で復号し
m1を取得
S705
アクセスチケット生成検証
補助データd111取得
S706
S707
m1=(id1,d111)なる
チケットID id1が有効アクセスチケット
情報に存在するか
NO
YES
S708
S709
有効と判定
無効と判定
(アクセスチケット検証手続き)
終了

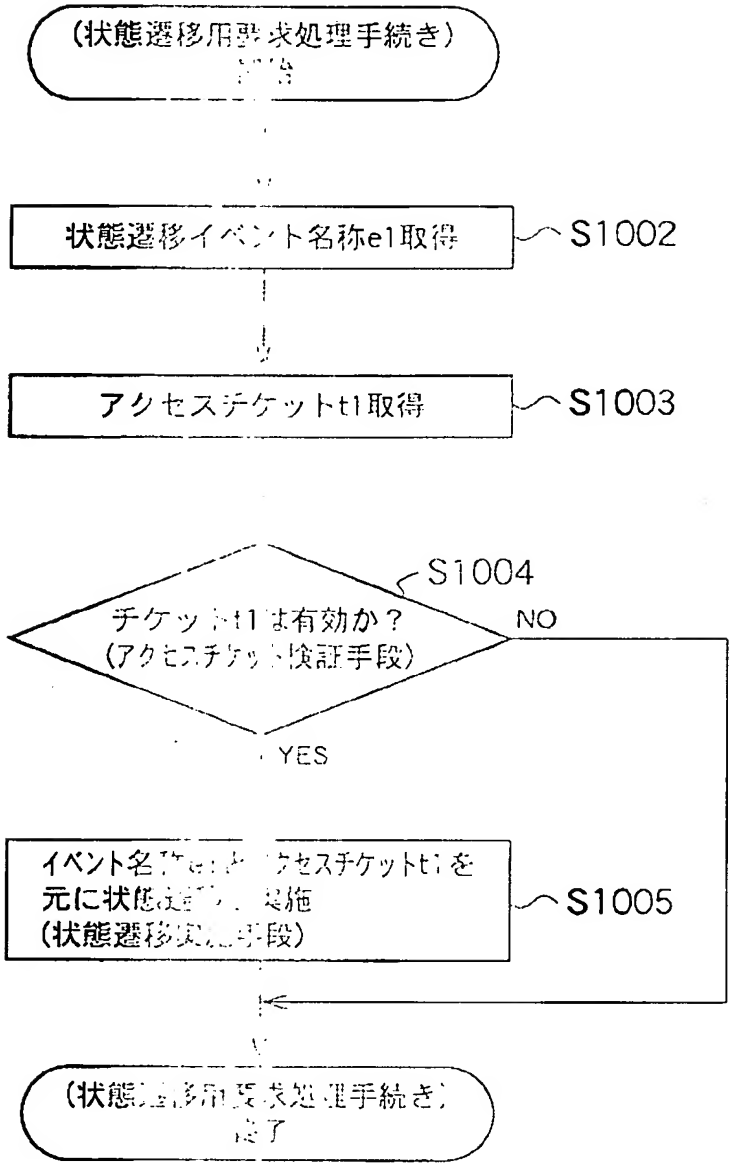
【図８】


(アクセス要求処理手続き)
開始
アクセス要求req1取得
S802
アクセスチケットt1取得
S803
S804
チケットt1は有効か？
(アクセスチケット検証手段)
NO
YES
S805
アクセス要求
req1を許可するか？
(アクセス権限判定手段)
NO
YES
アクセス要求req1を処理
S806
(アクセス要求処理手続き)
終了

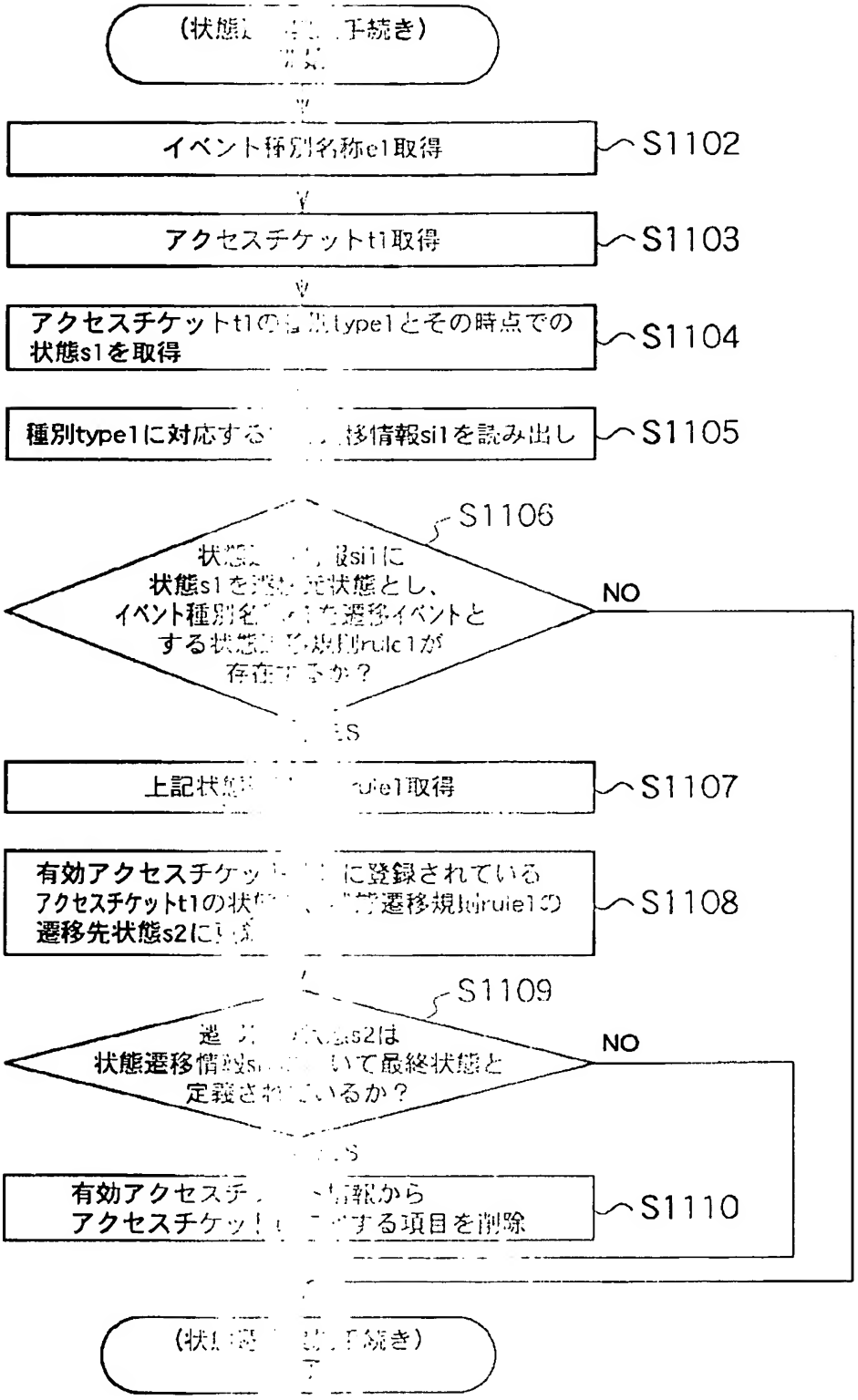
【図９】


開始
アクセス要求req1取得
S902
アクセスチケットt1取得
S903
S904
種別type1に対応する
S905
S906
S907
NO
YES
S908
S909
アクセス要求req1は不許可と判定
終了

【図10】



【図１１】



フロントページの続き

Ｆターム(参考) 5B017 AA01 BA05 BA07
BB07 CA16
5B049 BB11 CC02 CC05
GG04 GG07 GG11
5B085 AA08 AE08 AE23
BE07 BG06
5J104 AA07 KA01 KA04 NA36 PA07 PA10
9A001 JJ18 JJ25 JZ67